GTA Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Use of Cryptography**	
PSG Number:	PS-08-024.01	**Topical Area:** Security
Document Type:	Policy	**Pages:** 2
Issue Date:	3/20/08	**Effective Date:** 3/20/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Where the confidentiality, authenticity, or integrity of information is critical, the use of cryptographic controls may be warranted.	

PURPOSE

Cryptography is a discipline that embodies principles, means and methods for providing several security services: confidentiality, data integrity, authentication and non-repudiation.

This policy establishes the requirement to use cryptographic controls on State information systems as necessary.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

POLICY

Agencies shall use cryptographic controls where the confidentiality, authenticity, non-repudiation or integrity of data is categorized MODERATE or higher or when the risk of compromise or exposure is higher than acceptable or when required by policy, law, or regulation, and other compensating controls are insufficient to meet the required security levels.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Implementing Cryptographic Controls (Standard)

REFERENCES

NIST SP 800-12 (chapter 19) Introduction to Computer Security NIST Handbook
NIST SP 800-21 Guideline for Implementing Cryptography in the Federal

Government
FIPS 140-2 Security Requirements for Cryptographic Modules
NIST Cryptographic Key Tool Kit http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html

TERMS and DEFINITIONS

Cryptography is a branch of applied mathematics concerned with encrypting and decrypting data such that the sender's identity (authentication and non-repudiation), data confidentiality or integrity can be assured.

- **Encryption** is the process of converting ordinary information (plaintext) into unintelligible character strings (i.e., *ciphertext*).
- **Decryption** is the reverse, moving from unintelligible ciphertext to plaintext.
- A **cipher** (or *cypher*) is a pair of algorithms which perform this encryption and the reversing decryption.

Non-Repudiation is a service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party.

Authentication is a process that establishes origin of information or determines an entity's identity.

Note: The PSG number was changed from P-08-024.01 on September 1, 2008.